FINANCIAL™
DATA EXCHANGE

The ABC's of APIs

ORGANIZATION OVERVIEW

Table of Contents

A. Why share financial data?

Digital technologies are providing new and different ways for financial institutions, financial technology (fintech) companies, and others to support the financial needs of consumers and businesses through innovative products, services, and applications (apps). These solutions often require access to financial data to benefit the end user, for example, by presenting a holistic view of the user's finances to help them make better spending decisions or by using the user's data to make a decision on whether or not to offer them a loan.

B. How do financial apps get the data?

First and foremost, financial apps must disclose to the user which data is required and how it will be used. Once the user's consent (consent is described in greater detail within the Appendix of this document) is obtained, the financial apps may then gather the information on the user's behalf, generally in one of two primary ways: screen scraping or Application Programming Interfaces (APIs).

C. What is screen scraping?

Screen scraping is the process of collecting screen display information (i.e. the text that appears on a website) for the purposes of another application. For example, knowing that online banking websites display a customer's financial records such as balances and transactions, this data can be retrieved by downloading all of the information presented on the banking website and knowing which elements represent the balances and transactions.

The following example describes how a consumer's financial data gets into a financial app by way of screen scraping:

1

THE PLAYERS

Janet is the new user of MyMoney.

MyMoney is a new Financial App on the web.

Bank ABC holds several of Janet's accounts.

Figure 1. The main players in this example

2

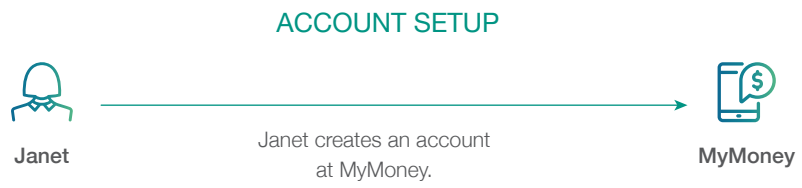

Figure 2. Account Setup with a financial app

3

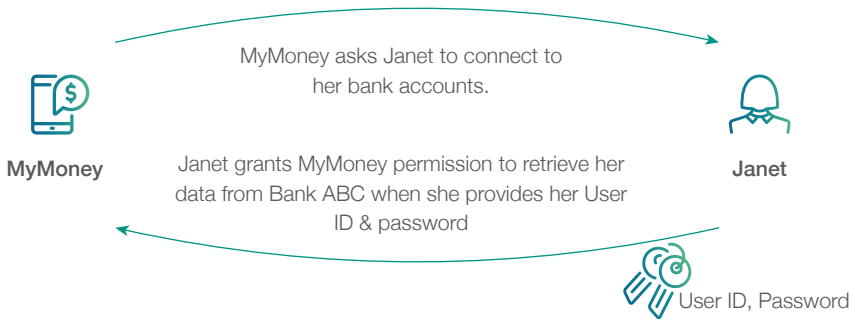

Figure 3. Credential sharing with a financial app

Figure 3:

1. MyMoney asks Janet to connect her bank accounts.
2. Janet indicates that she holds accounts at Bank ABC.
3. MyMoney requests Janet's User ID and Password to Bank ABC so that it can retrieve her financial data on her behalf (a User ID and Password are also called credentials - see the following section for more information about credentials and why they are important for accessing financial apps).
4. Janet grants MyMoney permission to retrieve her data by providing MyMoney with her User ID and Password to Bank ABC.
5. MyMoney stores Janet's User ID and Password so that it can maintain up-to-date information for Janet.

4

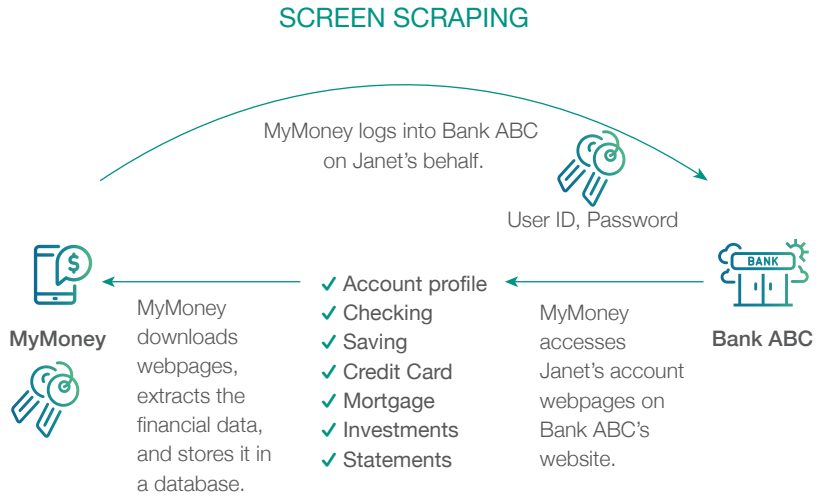

Figure 4. FinTech screen scraping a bank

Figure 4:

1. MyMoney logs into Bank ABC's website using Janet's User ID & password.
2. MyMoney stores Janet's financial data in its databases.

D. What are credentials and what is credential sharing?

Credentials are what Janet uses to prove to a computer system or app that she is who she says she is. In this example, the User ID and Password that Janet uses to log into her bank's website are her credentials. In general, credentials are used to authenticate an individual and may include: something you are (e.g., a finger-print), something you know (e.g., a password), or something you have (e.g., a passcode sent to your phone).

When Janet enrolls with some financial apps, they will ask her for the User ID and Password she uses to log into her bank. This is so that they can log into the bank on her behalf, download her balances and transactions, and provide her with up-to-date and uninterrupted services on an ongoing basis. In this case, Janet is sharing her bank credentials with the financial app, which will store her credentials using security precautions.

Key points to know:

1. The app can retrieve a consumer's data from their bank whenever or as often as it needs. Because it has the consumer's credentials it can access data beyond what the consumer might think the app needs.
2. The app can continue to retrieve a user's data until they change their credentials or until they terminate the app's permissions. Deleting a financial app from one's phone or PC does not stop the app from continuing to collect data from the consumer's bank account.
3. Another company now has credentials, adding another place where information can be stolen.

E. Does each app do its own screen scraping?

No, most of the thousands of financial apps use a small number of companies called aggregators to collect data for them. For simplicity, the example here focuses only on the app and the customer, though it should be noted that there is usually an aggregator in between.

F. Are there challenges with screen scraping?

For example, when a bank updates its online banking page, a financial app can't collect the same data in the same way. In this case, Janet may notice that MyMoney hasn't completely updated her balances and transactions from Bank ABC or that the information may be inaccurate.

To address this and other challenges, companies have gotten together to introduce and implement API standards.

G. What is an API?

API stands for Application Programming Interface. It's a fancy way of referring to a method for computers to talk to one another using a common format.

APIs make sharing data easier, more accurate and more secure because they lay out, in detail, the rules for how to request data and what data will be returned.

Financial services companies and industry groups have formed the Financial Data Exchange and have created a set of standards for sharing data known as the FDX API 3.0. It lays out rules for how to request data, what data will be returned, in what format and how it will be encrypted. Complying with standards helps all participants share data in a meaningful, secure and convenient way.

How the FDX API works

Let's say two companies want to share account and transaction information for Janet. Using the FDX API, they know how to request data and what it will look like coming back. The conversation between two computer systems might look like this if they were using the FDX API:

Financial App: Hi, Bank ABC, I'm looking for all of Janet's available accounts.
Bank ABC: Here is a list of her accounts: 1, 2, 3, 4, 5.
Financial App: For account 1, can I get her account details?
Bank ABC: Account 1 is a checking account with current balance of $100.
Financial App: For account 1, can I get transactions for the last 7 days?
Bank ABC: Account 1 had 10 transactions:
1) Check 1091 for $20 on May 5th
2) ATM withdrawal for $30 on May 6th
3) etc. ….

APIs allow apps to borrow functionality and data from one another and become reusable building blocks to new apps. For example, Uber leverages several APIs to offer its service, including payment apps such as PayPal to pay its drivers, Google Maps to pin point where drivers and passengers are, and instant messaging APIs to communicate with them.

H. How many banks and financial apps are using the FDX API?

As of February 2019, 93% of FDX member firms surveyed reported either being in production with the FDX API or were in some stage of 2019 planning, developing, or deploying the FDX API. These are many of the largest banks and aggregators.

View the current FDX member list here: *https://financialdataexchange.org/pages/members*

I. What is the difference between an API and screen scraping?

We saw how screen scraping worked above in Figures 1-4. Below we will provide an example of how computers interact using an API. Figures 3 and 4 above can be contrasted with Figures 7 and 8 below.

An example using an API:

5

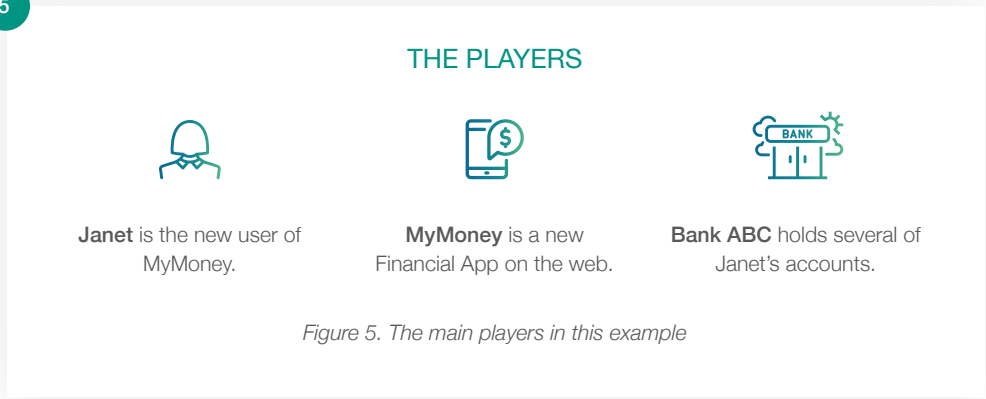

Figure 5. The main players in this example

6

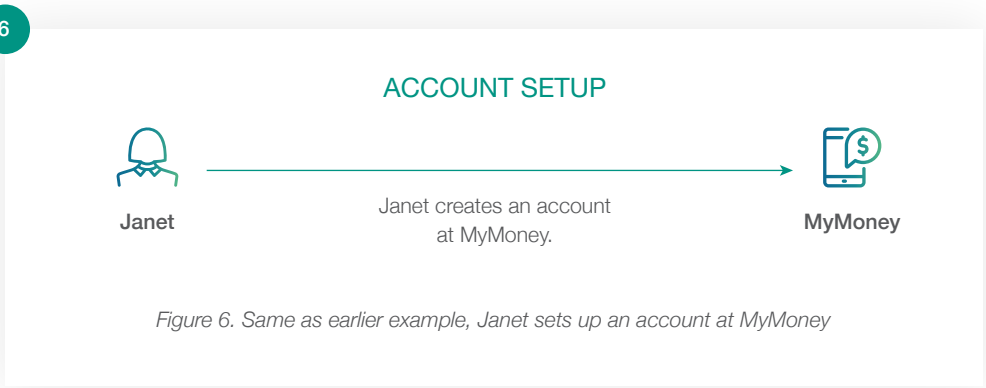

Figure 6. Same as earlier example, Janet sets up an account at MyMoney

7

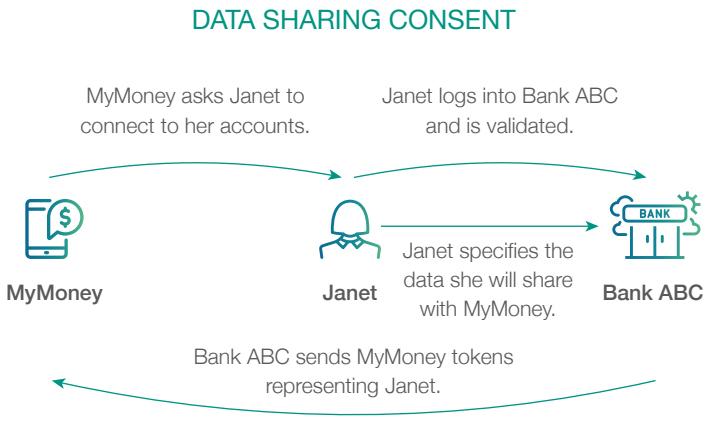

Figure 7. Data Sharing Authorization and Consent using an API

Figure 7:

1. MyMoney asks Janet to connect to her bank.
2. Janet picks Bank ABC from a list of banks.
3. MyMoney sends Janet to Bank ABC's authentication webpage (Janet is now on Bank ABC's website).
4. Janet logs into Bank ABC.
5. Bank ABC validates Janet's User ID and password and asks her:
   a. Which accounts she would like to share with MyMoney?
   b. What data she would like to share with MyMoney?
   c. Is she certain this is what she wants to do?
6. Janet confirms her choices.
7. Bank ABC sends Janet back to MyMoney with a token. (The token will identify Janet and her choices to Bank ABC but will contain no information useful to anyone else.)
8. MyMoney uses the token to retrieve Janet's accounts and transactions.

Please see the authentication workflow example in Figure 9 on page 10 below.

8

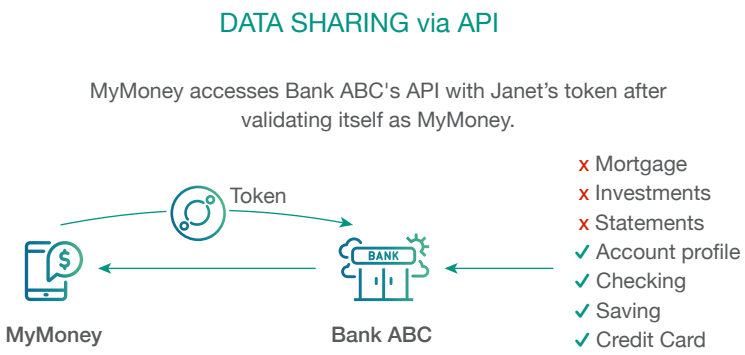

Figure 8. How data is retrieved using an API

Figure 8:

1. MyMoney validates or proves itself to Bank ABC.
2. MyMoney sends Janet's token to Bank ABC requesting data.
3. Bank ABC sends only the data Janet agreed to share with MyMoney.

J. Are there advantages to an API?

Designed to give consumers more control, APIs are considered more secure, more stable, more accurate and faster than screen scraping.

Control

When Janet consents to sharing data with a financial app, she can limit what data will be shared with MyMoney. Depending on the companies and apps, Janet may be able to specify what data to share (such as tax, banking, investment or insurance information) or which accounts. There are no easy ways to place limits on screen scraping.

Accuracy and Completeness

When companies implement APIs such as the FDX API, they are agreeing to make data available in a predictable manner. This allows apps like MyMoney to know in advance the data they can collect and the rules for collecting. This gives Janet the assurance that the Bank ABC data MyMoney collects and displays to her is accurate, complete, and current.

It also means that Janet won't have to share – and the app won't have to store – her credentials such as her User ID and password.

K. An Authentication Workflow Example

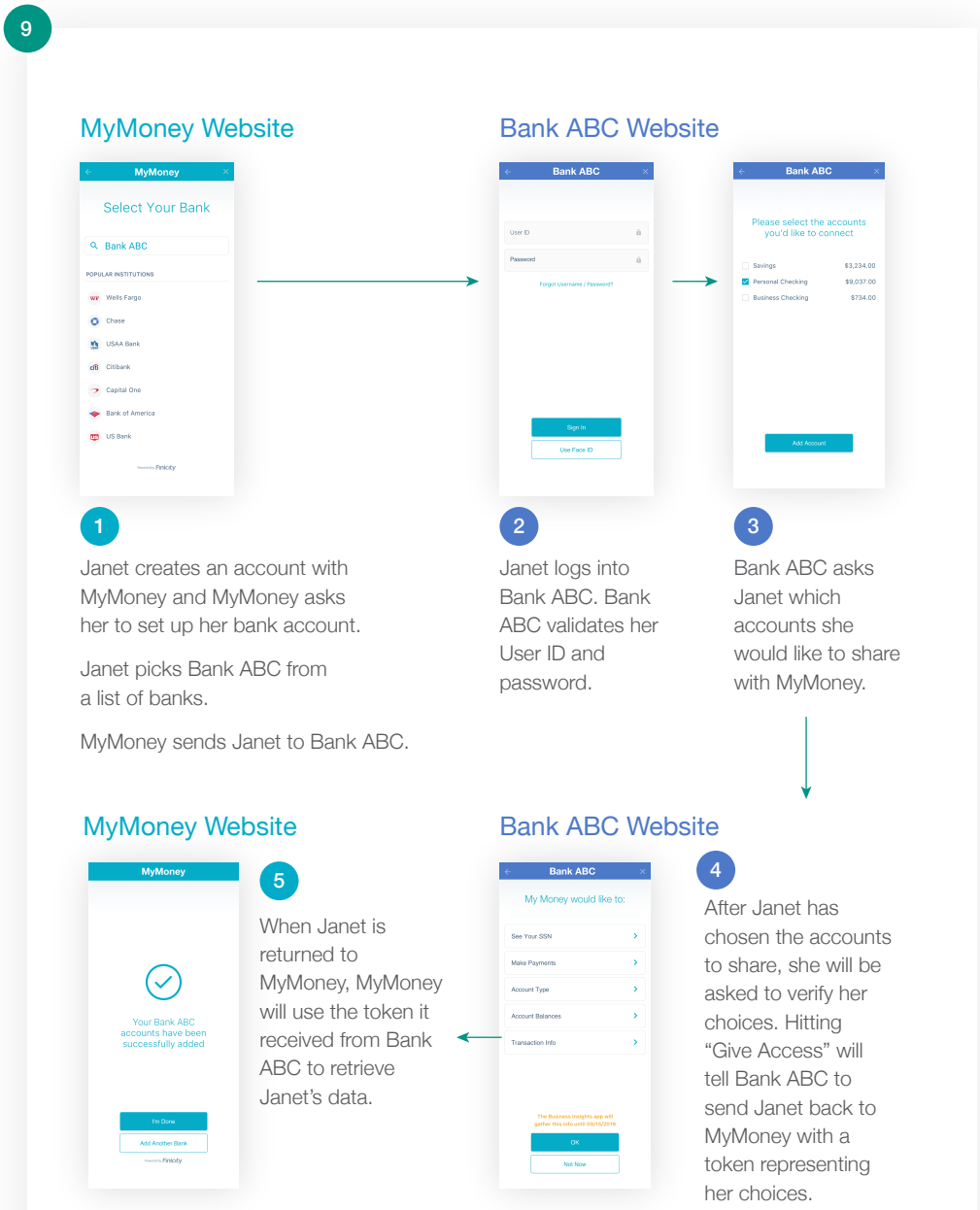

Figure 9. Authentication Workflow (See description of authentication in Appendix)

L. What is a token?

A token is a randomly generated string of characters up to 1,000 characters long. Bank ABC generates a token based on Janet's choices and sends it to MyMoney when Janet confirms her choices. This token is useful only to Bank ABC and MyMoney and only for Janet's data.

To everyone else, the token is a meaningless string. It contains no personally identifying information such as name, birthdate or Social Security Number. It also usually expires in a short period of time. MyMoney needs to regularly update or refresh the token with Bank ABC when seeking Janet's data. This makes tokens less useful to hackers.

The token provides all this security simply by Bank ABC and MyMoney using the same API, and Janet can relax knowing that only Bank ABC knows her User ID and password and they can't be stolen using a token.

Appendix: Technical Topics

A. What is Authentication?

Authentication is the process of verifying whether someone is who they say they are. Authentication methods control and grant access for systems by matching the user's credentials to their database. Example of authentication methods include:

- Something the user knows (such as a username or a password)
- Something the user has (such as a smart card or a phone)
- Something inherent to the user (such as a fingerprint or facial recognition)

When a user logs into an app using User ID and password, they are authenticating.

B. What is Authorization?

Authorization is the process of granting people, entities or apps access to a user's data. When a user fills out a mortgage or credit card app, she typically grants the lender access to her personal data so the entity can make a determination regarding her credit worthiness. Joint accounts are an example of shared authorization.

With APIs, consumers have the ability to specify which accounts they will share and, where applicable, what data they will share.

C. What is consent as it relates to sharing financial information?

Consent is when Janet instructs her bank to share her data with a third party. Options for specifying what data to share, when and for how long differ from bank to bank. Data cannot be shared without Janet's consent.

Consent is performed explicitly by the user (Janet). Janet gives express permission for Bank ABC to share data with MyMoney. As mentioned above, when Janet is connecting MyMoney to her bank (Bank ABC), she is redirected to the bank's website where she enters her User ID and password and validates herself to the bank.

Once validated, Bank ABC will present a series of options to Janet as to what data she wishes to share with MyMoney. (Note: the options vary among financial institutions.) The options can refer to accounts and types of data she wishes to share.

Bank ABC will make note of Janet's choices and only share the data Janet identified.

The last, and possibly most critical element of consent, is revocation (or reversal or termination of consent). Bank ABC provides Janet with the ability to revoke consent whenever she desires. Once consent is revoked, Janet's token at MyMoney is no longer valid and MyMoney no longer has access to Janet's data.